Managing Pod Through Cisco VIM Insight

The following topics tell you how to install and replace Cisco Virtual Infrastructure Manager (VIM) nodes using Cisco VIM Insight.

- Managing Hardware, page 1
- Managing Software, page 7
- Pod User Administration, page 22

Managing Hardware

Management of your Cisco VIM pods includes adding, removing, or replacing the nodes.

In a pod, multiple nodes cannot be changed at the same time. For example, if you want to replace two control nodes, you must successfully complete the replacement of the first node before you start to replace the second node. Same restriction applies for addition and removal of storage nodes. Only, in case of Compute Nodes you can add/remove multiple nodes together; however, there must always be one active compute node in the pod at any given point. VNF manager stays active and monitors the compute nodes thereby moving the VNFs accordingly as compute node management happens.

Note When you change a control, storage, or compute node in a Cisco VIM pod using Insight, it will automatically update the server and role in the active blueprint, as a result, your OpenStack deployment will change. When a node is removed from Cisco VIM, sensitive data may remain on the drives of the server. Administrator is advices to use Linux tools to wipe the storage server before using the same server for another purpose. The drives used by other application server should also be wiped out before being added to Cisco VIM.

Managing Storage Nodes

Before you add or remove a storage node, review the following guidelines for Managing Storage Nodes.

- **Required Number of Storage Nodes**: A Cisco VIM pod must have a minimum of three and a maximum of 20 storage nodes. If your pod has only two storage nodes, you cannot delete another storage node until you add another storage node. If you have fewer than three storage nodes, you can add one node at a time until you get to 20 storage nodes.

- **Validation of Nodes**: When you add a storage node to a pod, Cisco VIM Insight validates that all the nodes in the pod meet the minimum requirements and are in active state. If you have a control or compute node in a faulty state, you must either correct, delete or replace that node before you can add a storage node.
- **Update Blueprint**: When you add or delete a storage node, Insight will update the blueprint for the Cisco VIM pod.
- **Storage Node Logs**: You can access the logs for each storage node from the link in the Log column on the **Storage Nodes** tab.

Failed Addition or Deletion of Storage Node: If your attempt to add or delete a storage node fails, complete the following instructions:

Step 1 Choose the storage node in the list and click **Delete**.

Step 2 If the delete fails, click **Clear DB Entry** to remove the failed node from the database.
If you do not remove the node from the database, you cannot add another node to bring the number of nodes to three.

Adding Storage Node

You cannot add more than one storage node at a time. Complete the following instructions to add a storage node:

Before You Begin

- Remove the non-functional storage node from the pod. You can have maximum 20 storage nodes in a Cisco VIM pod.
- Ensure that the server for the new storage node is in powered state in OpenStack for C Series.

Step 1 In the navigation pane, choose **Post-Install** > **Pod Management**.

Step 2 Click the + icon next to **Sufficient Pool Present** next to **Add/Remove Storage Node**.

- Sufficient POOL check is automatically filled by Insight.
- It checks the number of IP present in the POOL for Management or Provision.
- If number of nodes is equal to pool size then the option would be disabled and you need to increase the pool size by clicking + icon.
- Validation check to see if the IP is valid and belongs to the same subnet of the existing IP Pool are applied by insight before you add IPs to Management/Provision network.

Step 3 For C Series, add the following details:

- **Server Name**: Name for the Storage Server to be added.
- **Rack ID**: Enter the Rack ID. (Accepts String format).
- **CIMC IP**: Enter the CIMC IP.
- **CIMC User Name**: User name for the CIMC.
- **CIMC Password**: Enter the password for the CIMC
- **VIC Slot**: Enter the VIC Slot (Optional).
- **ToR switch info**:Mandatory if ToR is configured as True
  - **Management IPv6**: Enter IPv6 Address.

Step 4 For B Series, add the following details:

- **Server Name**: Name for the Storage Server to be added.
- **Rack ID**: Enter the Rack ID. (Accepts String format).
- **Rack Unit ID**: Enter the Rack Unit ID.
- **Management IPv6**: Enter IPv6 Address.

If all mandatory fields are filled in correctly then **Add Storage** button will be enabled.

Step 5 Click **Add Storage**. Add node initialized message will be displayed.

Step 6 To view logs, click **View logs** under Logs column.
The status of the POD will change to Active.

Step 7 Two kinds of failure may occur:

- **Add Node Pre-Failed**: When addition of node failed before the bare-metal stage (step 4) the Active Blueprint will be modified but the Node is not yet added in the Cloud. If you press **X** Icon, then Insight will delete the node information form the Blueprint and the state would be restored.
- **Add Node Post-Failed**: When addition of node failed after the bare-metal stage (step 4) the Active Blueprint will be modified and the node is registered in the cloud. If you press **X** Icon, then Insight will first delete the node from the Blueprint and then node removal from cloud would be initiated.

You can view the logs for this operation under **Logs** column.

Deleting Storage Node

You cannot delete more than one storage node at a time.

Step 1 In the Navigation pane, choose **Post-Install** > **POD Management**.

Step 2 Click **X** adjacent to the storage node you want to delete.

Step 3 **Node Removal Initiated successfully** message will be displayed.
To view logs, click **View logs** under logs column.

- If the Storage Node is deleted successfully, the storage node will be removed from the list under **Add/Remove storage Node**.
- In deletion failed, a new button **Clear Failed Nodes** will be displayed. Click **Clear Failed Nodes** to remove the node form cloud and Blueprint.

Managing Compute Nodes

Before you add or remove a compute node, review the following guidelines:

- **Required Number of Compute Nodes**: A Cisco VIM pod must have a minimum of one compute node and a maximum of 96 compute nodes. If your pod has only one compute node, you cannot delete that node until you add another compute node.
- **Update Blueprint**: When you add or remove a compute node, Insight will update the blueprint for the Cisco VIM pod.
- **Compute Node Logs**: You can access the logs for each compute node from the link in the Log column on the Compute Nodes table.

Adding Compute Node

Complete the instructions, to add a compute node:

Before You Begin

Ensure that the server for the new compute node is in powered state in OpenStack. You can add more than one compute node at a time.

Step 1 In the navigation pane, click **Post-Install** > **Pod Management**.

Step 2 Click + icon next to **Sufficient Pool Present** adjacent to **Add/Remove Compute Node**.

- Sufficient POOL check is automatically filled by Insight.
- It checks the number of IP present in the POOL for Management or Provision.

- If number of nodes is equal to pool size then the option would be disabled and you need to increase the pool size by clicking + icon.
- Validation check to see if the IP is valid and belongs to the same subnet of the existing IP Pool are applied by insight before you add IPs to Management/Provision network.

Step 3 For C Series, add the following details:

- **Server Name**: Name for the Compute Server.
- **Rack ID**: Enter the Rack ID. (Accepts String format).
- **CIMC IP**: Enter the CIMC IP.
- **CIMC User Name**: User name for the CIMC.
- **CIMC Password**: Enter the password for the CIMC.
- **VIC Slot**: Enter the VIC Slot (Optional).
- **ToR switch info**: Mandatory if configured ToR is true.
- **DP ToR switch info**: Enter input as string format.
- **SRIVO ToR info** : Enter input as string format.
- **Management IPv6** : Enter IPv6 Address.

Step 4 For B Series, add the following details:

- **Server Name**: Name for the Storage Server to be added.
- **Rack ID**: Enter the Rack ID. (Accepts String format).
- **Rack Unit ID**: Enter the Rack Unit ID.
- **Chassis ID**: Enter the Chassis ID. Range for Chassis ID is 1-24.
- **Blade ID**: Enter the Blade ID. Range for Blade ID is 1-8.
- **CIMC Password**: Enter the CIMC Password.
- **Management IPv6**: Enter IPv6 address.

  If all mandatory fields are filled in correctly then click **Save**

Note Add Compute process can initiate multiple add of compute nodes. Fill in the mandatory fields to save new compute node or press cancel to exit message will be displayed.

Fields of Pod management will remain mandatory for user input based on setup-data.

Step 5 You may perform one among these steps mentioned below:

- Clicking **Cancel** displays the compute node information listed in the table and **Add Compute Node** button is enabled.
- If you feel you have filled in a wrong entry for the compute node information, click **Delete**. This will delete the entry from the table as this information is not added in the Blueprint.
- Click **Add Compute**, displays Add node initialized message.

Step 6 To view logs, click **View logs** under Logs column. The status of the POD will change to Active.

Step 7 Two kinds of failure may occur:

- **Add Node Pre-Failed**: When addition of node failed before the bare-metal stage (step 4) the Active Blueprint will be modified but the Node is not yet added in the Cloud. If you press **X** Icon, then Insight will delete the node information form the Blueprint and the state would be restored.
- **Add Node Post-Failed**: When addition of node failed after the bare-metal stage (step 4) the Active Blueprint will be modified and the node is registered in the cloud. If you press **X** Icon, then Insight will first delete the node from the Blueprint and then node removal from cloud would be initiated.

You can view the logs for this operation under **Logs** column.

Deleting Compute Node

Compute node is deleted due to a hardware failure. You can delete one compute node at a time.

Note If your pod has only one compute node, you cannot delete that node until you add another compute node.

Step 1 In the navigation pane, choose **Post-Install** > **POD Management**.

Step 2 Click **X** for the compute node to be deleted.
Node Removal Initiated successfully message will be displayed.

Step 3 To view the logs, click **View logs** under Logs column.

- If compute nodes are deleted successfully, you will not be able to view the compute node in the list under **Add/Remove Compute Node**.
- If deletion has failed, a new button **Clear Failed Nodes** will be visible.

Step 4 Click **Clear Failed Nodes** to remove the node form Cloud and Blueprint.

Managing Control Nodes

Before you replace a control node, review the following guidelines:

- **Required Number of Control Nodes**: A Cisco VIM pod must have three control nodes and you can only replace one node at a time.
- **Validation of Nodes**: When you replace a control node, Cisco VIM Insight validates if all the other nodes in the pod meet the minimum requirements and are in active state. If you have a storage or compute node in a faulty state, you must correct the faulty state or delete or replace that node before you can replace the control node.

- **Update Blueprint**: When you replace a control node, Insight will update the Active blueprint for the Cisco VIM pod.
- **Control Node Logs**: You can access the logs for each control node from the link in the **Logs** column of Control Nodes table.

Replacing Control Node

You can replace only one control node at a time.

Step 1 In the Navigation pane, click **Post-Install** > **Pod Management**.

Step 2 Click **Edit/Replace** under the Action column of the **Replace Control** table.

Step 3 On success, **Replace Node Initiated** successfully message will be displayed.

Step 4 You can view the logs in the **Logs** column on the Control Nodes table.

What to Do Next

If the replacement of the control node fails, do the following:

- Click on the link in the Logs column.
- Check the logs to determine the cause of the failure.
- Correct the issue and attempt to replace the control node again.

Managing Software

Software management of your Cisco VIM pods includes software update, reconfigure of openstack services and password, etc.

VIM Software Update

As part of the lifecycle management of the cloud, VIM has the ability to bring in patches (bug fixes related to code, security, etc.), thereby providing cloud management facility from software point of view. Software update of the cloud is achieved by uploading a valid tar file, following initiation of a System Update form the Insight as follows:

Step 1 In the Navigation pane, click **Post-Install** > **System Update**.

Step 2 Click **Browse** and select the valid tar file.

Step 3 Click **Open**.

Step 4 Click **Upload and Update**.
Update started Successfully message will be displayed.

Step 5 Update status will be shown as **ToUpdate**.
Click the hyperlink to view the reconfigure logs for install logs.

Reconfigure status will be available on the page or the dashboard under **POD Operation** details.

What to Do Next

System Update has been initiated message will be displayed. Logs front-ended by hyperlink will be in the section below in-front of **Update Logs** which shows the progress of the update. During the software update, all other pod management activities will be disabled. Post-update, normal cloud management will commence. Once update has completed you will see the status of update in the box below.

If log update fails, **Auto-RollBack** will be initiated automatically.

If log update is Successful, you will have two options to be performed:

1. **Commit—**To proceed with the update.
2. **RollBack—**To cancel the update.

If Auto-rollback fails during software update fails through Insight UI, it is advised that the administrator contact Cisco TAC for help. Do not re-try the update or delete the new or the old installer workspace.

Reconfigure Password

- **Regenerate all passwords**: Click **Regenerate all passwords** checkbox and click **Set Password**. This will automatically regenerate all passwords in alphanumeric format.
- **Regenerate single or more password**: This will set a specific password by doing an inline edit for any service like Horizon's ADMIN_USER_PASSWORD. Double click on the filed under Password and enter the password to enable **Set Password** button.

During the reconfiguration of password, all other pod management activities will be disabled. Post-update, normal cloud management will commence. If the reconfigure of the password fails, all subsequent pod management operations will be blocked. It is advised to contact Cisco TAC to resolve the situation through CLI.

Reconfigure OpenStack Services, TLS Certificates and ELK Configurations

Cisco VIM supports the reconfiguration of OpenStack log level services, TLS certificates, and ELK configuration. Listed below are the steps to reconfigure the OpenStack and other services:

Step 1 In the Navigation pane, click **Post-Install** > **Reconfigure Openstack Config**.

Step 2 Click on the specific item that you want to change and update. For example: to update TLS certificate click the path to certificate location.

Step 3 Enter **Set Config** to commence the process.

What to Do Next

During the reconfiguration process, all other pod management activities will be disabled. Post-update, normal cloud management will commence. If reconfigure of OpenStack Services fail, all subsequent pod management operations will be blocked. It is advised to contact Cisco TAC to resolve the situation through CLI.

Reconfiguring CIMC Password

Cisco VIM Insight offers to reconfigure CIMC Password only for C Series Management Node. In case of B Series Management node the navigation menu to reconfigure the CIMC Password link will not be visible.

You need to match the following Password rule to run Reconfigure of CIMC Password:

- Must contain at least one lower case letter.
- Must contain at least one upper case letter.
- Must contain at least one digit between 0 to 9.
- One of these special characters !$#@%^-_+=*&
- Your password has to be 8 to 14 characters long.

Step 1 Log-in to **CISCO VIM Insight**.

Step 2 In the navigation pane, select **Post-Install**.

Step 3 Click **Reconfigure CIMC Password**.

Step 4 You can reconfigure the CIMC Password at global level by adding new CIMC_COMMON Password or to reconfigure CIMC Password for individual servers double click the server password you want to edit.

Step 5 Click **Reconfigure**to initiate reconfigure process.

Reconfigure Optional Services

Cisco VIM offers optional services such as heat, migration to Keystone v3, NFVBench, NFVIMON, etc, that can be enabled post-pod deployment. These services can be enabled in one-shot or selectively.

Listed below are the steps to enable optional services:

Step 1 In the Navigation pane, click **Post-Install** > **Reconfigure Optional Services**.

Step 2 Choose the right services and update the fields with the right values.

Step 3 Click **Offline validation**. Once offline validation is successful.

Step 4 Click **Reconfigure** to commence the process.
During the reconfiguration process, all other pod management activities will be disabled. Post-update, normal cloud management will commence.

If reconfigured OpenStack Services fail, all subsequent pod management operations are blocked. Contact Cisco TAC to resolve the situation through CLI.

Note All reconfigure operation feature contains repeated deployment true or false.

- Repeated re-deployment true - Feature can be re-deployed again.
- Repeated re-deployment false- Deployment of feature allowed only once.

Deployment Status :

Optional Features	Repeated re-deployment Option
APICINFO	True
EXTERNAL_LB_VIP_FQDN	False
EXTERNAL_LB_VIP_TLS	False
INSTALL_MODE	True
HTTP_PROXY & HTTPS_PROXY	True
LDAP	True
NETWORKING	True
NFVBENCH	False
NFVIMON	False
PODNAME	False
PROVIDER_VLAN_RANGES	True
SWIFTSTACK	True
SYSLOG_EXPORT_SETTINGS	False
TENANT_VLAN_RANGES	True
TORSWITCHINFO	False
VIM _ ADMINS	True
VMTP	False
VTS_PARAMETERS	False

Optional Features	Repeated re-deployment Option
AUTOBACKUP	` True
Heat	False
Keystone v3	False

Reconfiguring Optional Features through Insight

Step 1 Log-in to Cisco VIM Insight.

Step 2 In the **Navigation** pane, expand the **Post-Install Section**.

Step 3 Click **Reconfiguring Optional Feature through Insight**.

Step 4 On the **Reconfiguring Optional Feature through Insight** page of the Cisco VIM Insight, complete the following fields:

Name	Description
Heat checkbox	• Enable **Heat**. • Click **Offline Validation** . • Once Offline Validation is successful, click **Reconfigure** to commence the process..
Keystone v3 checkbox	• Enable **Keystone v3**. • Click **Offline Validation** . • Once Offline Validation is successful, click **Reconfigure** to commence the process.
ENABLE_ESC_PRIV	• Enable **ENABLE_ESC_PRIV** . • Click **Offline Validation** . • Once Offline Validation is successful, click **Reconfigure** to commence the process.

Name	Description
Autobackup checkbox	• Enable/Disable **Autobackup**. • Click **Offline Validation** . • Once Offline Validation is successful, click **Reconfigure** to commence the process.
External LB VIP TLS checkbox	• Enable **External LB VIP TLS**. • Click **Offline Validation** . • Once Offline Validation is successful, click **Reconfigure** to commence the process.
External LB VIP FQDN checkbox	• Enter Input as string. • Click **Offline Validation** . • Once Offline Validation is successful, click **Reconfigure** to commence the process.
Pod Name	• Enter Input as string. • Click **Offline Validation** . • Once Offline Validation is successful, click **Reconfigure** to commence the process.
Tenant Vlan Ranges	• Augment tenant vlan ranges input eg. 3310:3315. • Click **Offline Validation** . • Once Offline Validation is successful, click **Reconfigure** to commence the process.
Provider Vlan Ranges	• Enter input to tenant vlan ranges eg. 3310:3315. • Click **Offline Validation** . • Once Offline Validation is successful, click **Reconfigure** to commence the process.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><b>Install Mode</b></td><td>• Select <b>Connected</b> or <b>Disconnected</b>, any one form the drop-down list.
• Click <b>Offline Validation</b> .
• Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.</td></tr>
<tr><td><b>Syslog Export Settings</b></td><td>Following are the options for Skylog Settings:
<table>
<tr><td><b>Remote Host</b></td><td>Enter Syslog IP Address.</td></tr>
<tr><td><b>Facility</b></td><td>Defaults to local5</td></tr>
<tr><td><b>Severity</b></td><td>Defaults to debug</td></tr>
<tr><td><b>Clients</b></td><td>Defaults to ELK</td></tr>
<tr><td><b>Port</b></td><td>Defaults to 514 but can be modified by the User.</td></tr>
<tr><td><b>Protocol</b></td><td>Supports only UDP</td></tr>
</table>
• Click <b>Offline Validation</b> .
• Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.</td></tr>
<tr><td><b>Configure ToR</b> checkbox</td><td><b>True</b> or <b>False</b>. Default is false.</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><b>ToR Switch Information</b></td><td>Click + to add information for ToR Switch.
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td><b>Name</b></td><td>ToR switch name.</td></tr>
<tr><td><b>Username</b></td><td>ToR switch username.</td></tr>
<tr><td><b>Password</b></td><td>ToR switch Password.</td></tr>
<tr><td><b>SSH IP</b></td><td>ToR switch SSH IP Address.</td></tr>
<tr><td><b>SSN Num</b></td><td>ToR switch ssn num. output of show license host-id.</td></tr>
<tr><td><b>VPC Peer Keepalive</b></td><td>Peer Management IP. You need not define if there is no peer.</td></tr>
<tr><td><b>VPC Domain</b></td><td>Need not define if there is no peer.</td></tr>
<tr><td><b>VPC Peer port</b></td><td>Interface for vpc peer ports.</td></tr>
<tr><td><b>VPC Peer VLAN Info</b></td><td>vlan ids for vpc peer ports (optional).</td></tr>
<tr><td><b>BR Management Port Info</b></td><td>Management interface of build node.</td></tr>
<tr><td><b>BR Management PO Info</b></td><td>Port channel number for management interface of build node.</td></tr>
</table>
Click <b>Save</b>
• Click <b>Offline Validation</b> .
• Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.</td></tr>
</table>

Note When setup data is ACI VLAN with TOR then reconfigure options are
:

<table>
<tr>
<td><b>TORSwitch Information</b> mandatory table if you want to enter ToR information</td>
<td>Click + to add information for ToR Switch.
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Host Name</td><td>ToR switch name.</td></tr>
<tr><td><b>VPC Peer Keepalive</b></td><td>Peer Management IP. Do not define if there is no</td></tr>
<tr><td><b>VPC Domain</b></td><td>Do not define if there is no</td></tr>
<tr><td><b>Node ID</b></td><td>Integer, unique across all switches</td></tr>
</table>
Click <b>Save</b>
<ul>
<li>Click <b>Offline Validation</b> .</li>
<li>Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.</li>
</ul>
</td>
</tr>
<tr>
<td><b>NFV Bench</b></td>
<td>Enable checkbox which by default is false.
Add Tor info connected to switch:
<ul>
<li>Select a TOR Switch and Enter the Switch name.</li>
<li>Enter the port number. For example: eth1/5</li>
<li>NIC Ports: INT1 and INT2 optional input, enter the 2 port numbers of the 4-port 10G Intel NIC at the management node used for NFVBench.</li>
<li>Click <b>Offline Validation</b> .</li>
<li>Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.</li>
</ul>
<b>Note</b> If ToR is already present in Setup-data or already deployed. Then no need add Tor info, by default ToR info switchname will be mapped in NFV bench.
</td>
</tr>
</table>

<table>
<tr>
<td><b>Swiftstack</b>
SwiftStack is only supported with Keystone v2. If you select Keystone v3, swiftstack will not be available for configuration.</td>
<td>
<table>
<tr><td><b>Cluster End Point</b></td><td>IP address of PAC (proxy-account-container) endpoint.</td></tr>
<tr><td><b>Admin User</b></td><td>Admin user for swift to authenticate in keystone.</td></tr>
<tr><td><b>Admin Tenant</b></td><td>The service tenant corresponding to the Account-Container used by Swiftstack.</td></tr>
<tr><td><b>Reseller Prefix</b></td><td>Reseller_prefix as configured for Keysone Auth,AuthToken support in Swiftstack E.g KEY_</td></tr>
<tr><td><b>Admin Password</b></td><td>swiftstack_admin_password</td></tr>
<tr><td><b>Protocol</b> drop-down list</td><td>http or https</td></tr>
</table>
<ul>
<li>Click <b>Offline Validation</b> .</li>
<li>Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.</li>
</ul>
</td>
</tr>
</table>

<table>
<tr>
<td><b>LDAP with Keystone v3</b></td>
<td>
<table>
<tr><td><b>Domain Name</b> field</td><td>Enter name for Domain name.</td></tr>
<tr><td><b>Object Class for Users</b> field</td><td>Enter a string as input.</td></tr>
<tr><td><b>Object Class for Groups</b></td><td>Enter a string.</td></tr>
<tr><td><b>Domain Name Tree for Users</b></td><td>Enter a string.</td></tr>
<tr><td><b>Domain Name Tree for Groups</b> field</td><td>Enter a string.</td></tr>
<tr><td><b>Suffix for Domain Name</b> field</td><td>Enter a string.</td></tr>
<tr><td><b>URL</b> field</td><td>Enter a URL with ending port number.</td></tr>
<tr><td><b>Domain Name for Bind User</b> field</td><td>Enter a string.</td></tr>
<tr><td><b>Password</b> field</td><td>Enter Password as string format.</td></tr>
<tr><td><b>User Filter</b></td><td>Enter filter name as string.</td></tr>
<tr><td><b>User ID Attribute</b></td><td>Enter a string.</td></tr>
<tr><td><b>User Name Attribute</b></td><td>Enter a string.</td></tr>
<tr><td><b>User Mail Attribute</b></td><td>Enter a string.</td></tr>
<tr><td><b>Group Name Attribute</b></td><td>Enter a string.</td></tr>
</table>
<ul>
<li>Click <b>Offline Validation</b> .</li>
<li>Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.</li>
</ul>
</td>
</tr>
</table>

<table>
<tr>
<td><b>NFV Monitoring</b></td>
<td>Followings are the field values for NFV Monitoring:
<table>
<tr><td><b>Master</b> Admin IP field.</td><td>Enter Input as IP format.</td></tr>
<tr><td><b>Collector</b> Management IP field</td><td>Enter Input as IP format.</td></tr>
<tr><td>Collector VM1 info</td><td></td></tr>
<tr><td><b>Host Name</b> field</td><td>Enter Host Name as string.</td></tr>
<tr><td><b>CCUSER</b> password field</td><td>Enter Password.</td></tr>
<tr><td><b>Password</b> field</td><td>Enter password.</td></tr>
<tr><td><b>Admin IP</b> field</td><td>Enter Input as IP format.</td></tr>
<tr><td><b>Management IP</b> field</td><td>Enter Input as IP format.</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Collector VM2 info</td><td></td></tr>
<tr><td><b>Host Name</b>field</td><td>Enter a string.</td></tr>
<tr><td><b>CCUSER</b> field</td><td>Enter Password.</td></tr>
<tr><td><b>Management IP</b> field</td><td>Enter Input as IP format.</td></tr>
<tr><td></td><td></td></tr>
<tr><td><b>Dispatcher</b></td><td></td></tr>
<tr><td><b>Rabbit MQ Username</b> Field</td><td>Enter a string.</td></tr>
<tr><td></td><td></td></tr>
</table>

• Click <b>Offline Validation</b> .
• Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.
</td>
</tr>
<tr>
<td><b>VTS Parameter</b></td>
<td>Following are the fields to reconfigure for VTS parameters
<table>
<tr><td><b>VTC SSH Username</b> field.</td><td>Enter the string.</td></tr>
<tr><td><b>VTC SSH Username</b> field.</td><td>Enter the password.</td></tr>
</table>

• Click <b>Offline Validation</b> .
• Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.
</td>
</tr>
</table>

VMTP	

Check one of the check boxes to specify a VMTP network:

- Provider Network
- External Network

For the Provider Network complete the following:

Network Name field.	Enter the name for the external network.
IP Start field.	Enter the starting floating IPv4 address.
IP End field.	Enter the ending floating IPv4 address.
Gateway field	Enter the IPv4 address for the Gateway.
DNS Server field.	Enter the DNS server IPv4 address.
Segmentation ID field.	Enter the segmentation ID.
Subnet	Enter the Subnet for Provider Network.

For **External Network** fill in the following details:

Network Name field.	Enter the name for the external network.
Network IP Start field.	Enter the starting floating IPv4 address.
Network IP End field.	Enter the ending floating IPv4 address.
Network Gateway field	Enter the IPv4 address for the Gateway.
DNS Server field.	Enter the DNS server IPv4 address.
Subnet	Enter the Subnet for External Network.

<table>
<tr>
<td></td>
<td>• Click <b>Offline Validation</b> .
• Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.</td>
</tr>
<tr>
<td><b>Networking</b>
In Reconfigure optional services networking you can reconfigure IP tables, and/or add http_proxy/https_proxy.</td>
<td>To reconfigure networking, update the relevant information:
<table>
<tr><td><b>IP Tables</b></td><td>Click <b>Add(+)</b> to add table. Enter input as subnet format.
Eg. 12.1.0.1/2</td></tr>
<tr><td><b>http_proxy_server</b></td><td>Enter HTTP_PROXY_SERVER
Eg. <a.b.c.d:port></td></tr>
<tr><td><b>https_proxy_server</b></td><td>Enter HTTP_PROXY_SERVER
Eg. <a.b.c.d:port></td></tr>
</table>
• Click <b>Save</b>.
• Click <b>Offline Validation</b>.
• Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.</td>
</tr>
<tr>
<td><b>APICINFO</b>
<b>Note</b> Reconfigure optional services only APIC hosts can be reconfigure.</td>
<td>To reconfigure APICINFO, follow the process:
• Enter input for APIC hosts format. <ip1|host1>:[port] or eg.12.1.0.12
• Click <b>Save</b>.
• Click <b>Offline Validation</b>.
• Once Offline Validation is successful, click <b>Reconfigure</b> to commence the process.
<b>Note</b> APIC hosts can be reconfigure minimum 1 host and max 3 but not 2 hosts.</td>
</tr>
</table>

Vim_admins	To reconfigure vim_admins, follow the process: • To add a new root user, Click **+** and add the Username and admin hash password (Starting with $6). • To remove existing user, Click **-**. • Once Offline Validation is successful, click **Reconfigure** to commence the process.

Pod User Administration

Cisco VIM Insight offers Users (Pod Admin(s) or Pod Users) to manage Users and roles associated with them.

Managing Roles

To create a new Role

Step 1 Click **Login as POD User.**

Step 2 Navigate to **Pod User Administration** and click **Manage Roles**. By default you will see full-pod-access role in the table.

Step 3 Click **Add New Role** to create a new role.

Step 4 Complete the following fields in the **Add Roles** page in Cisco VIM Insight:

Field Name	Field Description
Role	Enter the name of the role.
Description	Enter the description of the role.
Permission	Check the **Permission** checkbox to select the permission.
Click **Save**.	Once the Blueprint is in Active state all the permissions are same for C-series and B-series PODs other than Reconfigure CIMC Password which is missing for B-series POD.

Note Permissions are divided in granular level where viewing **Dashboard** is the default role that is implicitly added while creating a role.

Managing Users

To add new User

Step 1 Click **Login as POD User**.

Step 2 Navigate to **POD User Administration**.

Step 3 Click **Manage Users**.

Step 4 Click **Add Users** to add a new user.

Step 5 Complete the following fields in the **Add Users** page of the Cisco VIM Insight:

Field Name	Field Description
Email ID	Enter the Email ID of the User.
User Name	Enter the User Name if the User is new. If the User is already registered to the Insight the User-Name gets auto-populated.
Role	Select the Role from the drop-down list.

Step 6 Click **Save**.

Managing Root CA Certificate

You can update the CA Certificate during the registration of the POD. Once, logged in as POD User and if you have the permission to update the certificate you can view under POD User Administration>> Manage Root CA Certificate.

To update the Certificate:

Step 1 Click **Login as POD User**

Step 2 Navigate to **POD User Administration>>Manage Root CA certificate**.

Step 3 Click **Browse** and select the certificate that you want to upload.

Step 4 Click **Upload.**

- If the certificate is Invalid, and does not matches with the certificate on the management node located at (var/www/mercury/mercury-ca.crt) then Insight will revert the certificate which was working previously.
- If the Certificate is valid, Insight will run a management node health check and then update the certificate with the latest one.

Note The CA Certificate which is uploaded should be same as the one which is in the management node.